Rethinking the PCI and SOC 2 delivery model: Specialization vs. integration in cybersecurity assurance SOC audits

Over the past decade, cybersecurity assurance has evolved from a niche compliance activity into a central pillar of enterprise trust. Customers, regulators, boards, and investors increasingly rely on independent reports, particularly Payment Card Industry Data Security Standard Reports on Compliance (PCI ROCs) and System and Organization Controls (SOC) 2 examinations, to evaluate how organizations safeguard sensitive data.

As demand has grown, so too has a debate within the market: Should organizations engage a single provider to deliver formal assessments over both PCI and SOC 2, or is it better to use separate firms specializing in each?

Both models have gained traction. Integrated cybersecurity assurance firms promote efficiency and coordination, while traditional professional services models emphasize specialization aligned with distinct professional disciplines. At KPMG, we believe this question deserves thoughtful consideration rather than a binary answer.

Understanding the fundamental differences

Although PCI ROCs and SOC 2 reports often appear side-by-side in vendor security questionnaires, they originate from fundamentally different frameworks and professional standards.

PCI Data Security Standard (DSS) assessments are rooted in cybersecurity operations with a very specific scope both in terms of the nature of testing and the in-scope assets. Related to the nature of testing, PCI assessors evaluate the highly technical implementation of prescriptive requirements designed to protect payment card data through the performance of up to 464 required, detailed test procedures. The accuracy of the assessment depends heavily on technical validation and deep familiarity with the prescribed DSS requirements. In terms of in-scope assets, because the PCI standard can be very expensive to apply, most organizations seek to limit the scope of the assessment to the smallest subset of assets possible through rigorous technological means. This is extremely difficult to achieve as PCI scoping rules generally favor zero connectivity between in-scope and out-of-scope systems, through any series of "hops."

SOC 2 examinations, by contrast, are grounded in the American Institute of Certified Public Accountants (AICPA) attestation standards that govern planning, execution, and reporting. These engagements assess whether controls effectively respond to risks that threaten the achievement of a service organizations objectives as evaluated against the AICPA trust services criteria. The service organization is responsible for stating their objectives and the boundaries of the system that is subject to the SOC 2 examination. The value of a SOC 2 report derives from assurance methodology, independence, evidence evaluation, and professional standards developed over decades within the technical accounting profession.

While the two reports intersect operationally, they remain distinct forms of assurance as well as scope.

The Rise of the integrated provider

Integrated assurance firms have emerged to meet organizations' desire for streamlined compliance programs. These providers argue that modern technology environments operate as unified control ecosystems. Identity management, cloud security, monitoring, and incident response capabilities underpin both PCI and SOC 2.

Their value proposition centers on several benefits:

- Reduced duplication of evidence requests
- Coordinated testing timelines
- Consistent control narratives/implementation descriptions across frameworks
- Lower administrative burden on management teams

There is theoretical merit to this perspective. Organizations understandably seek efficiency as assurance demands multiply.

Moreover, integrated firms have invested significantly in combining cybersecurity talent with attestation capabilities. The market's evolution reflects a broader convergence between technology risk and assurance disciplines.

Where integration meets its limits

However, efficiency alone does not define assurance quality, and PCI's difficult scoping rules often preclude real overlap.

The primary purpose of PCI and SOC 2 reporting is not operational convenience—it is external trust. These reports serve as independent validation relied upon by customers, regulators, auditors, and business partners. The credibility of that validation depends on the depth of expertise applied to each engagement.

Here, important distinctions emerge.

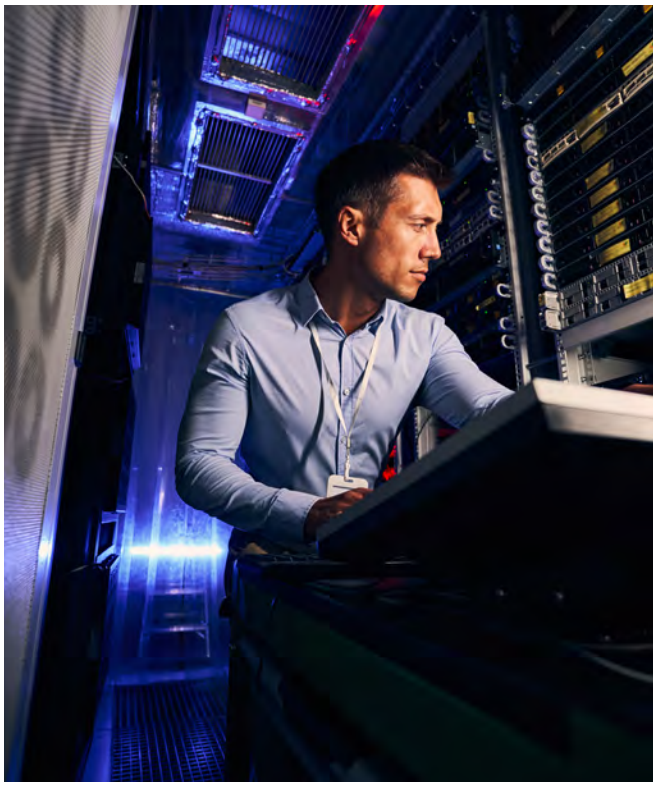
PCI assessments require professionals deeply embedded in technical cybersecurity practice, including experienced Qualified Security Assessors (QSAs) and Independent Security Assessors (ISAs) fluent in network architecture, threat detection, and real-world attack scenarios.

SOC 2 examinations demand a different institutional strength: disciplined attestation methodology supported by mature quality control systems, peer review processes, and professional skepticism ingrained through decades of assurance practice by experienced professionals including Certified Public Accountants (CPAs) that ultimately sign off on the reporting.

While integrated firms strive to excel across both domains, sustaining equal depth across two fundamentally different professional disciplines presents inherent challenges.

In addition, because PCI's scoping rules so heavily favor complete isolation between in-scope and out-of-scope systems, there are a separate set of security systems and controls dedicated to PCI environments. This separation helps prevent the "spread" of PCI and mitigates the risk that an attacker can, for example, compromise a configuration management server via an out-of-scope network, and use it to conduct an attack on an in-scope systems. Organizations that perceive a high degree of overlap in control enforcement mechanisms between their PCI and SOC2 environments may not have recently validated their PCI scope against the latest scoping rules and/or sufficiently limited their PCI scope.

Why professional heritage still matters



The accounting profession's role in assurance is not incidental. AICPA attestation standards evolved specifically to create consistent, defensible opinions relied upon by third parties. Longstanding CPA firms have built extensive infrastructure to support these engagements:

- Established independence frameworks
- Multi-level engagement quality reviews
- Robust risk management practices
- Peer and regulator reviewed assurance methodologies

These institutional capabilities underpin the trust associated with SOC reporting.

Similarly, specialized cybersecurity firms often maintain technical environments, tooling, and practitioner communities designed to keep pace with rapidly changing threats—capabilities particularly well suited to PCI validation.

Professional specialization exists for a reason: different disciplines require different forms of mastery.

The value of independent perspectives

From a governance standpoint, engaging separate firms for the formal PCI and SOC 2 assessments introduces a valuable dynamic to the extent the scope does overlap: independent professional perspectives applied to the same control environment.

Multiple assurance providers can:

- Challenge assumptions from different angles
- Reduce methodological blind spots
- Strengthen overall control maturity
- Enhance credibility with sophisticated stakeholders

This separation mirrors broader governance principles seen across financial reporting, internal audit, and risk oversight functions, where independence and diversity of review are viewed as strengths rather than inefficiencies.

Independent perspectives are so valued that many mature organizations not only hire a separate firm for PCI-related work, but rotate between PCI assessors every few years, to help ensure different perspectives are taken.

Market signals from mature organizations

Observing how mature enterprises structure assurance programs offers useful insight. Many large organizations increasingly adopt a differentiated approach:

- Technical cybersecurity specialists perform highly technical validations, including PCI-related work.
- Established public accounting firms issue SOC reports grounded in attestation standards.

This model reflects an understanding that different trust signals require different professional competencies.

Integrated providers remain attractive, particularly for high-growth companies seeking rapid certification cycles and/or where there is significant overlap between PCI and SOC 2 scope. However, organizations facing heightened regulatory scrutiny or complex stakeholder expectations often prioritize defensibility and credibility over operational simplicity.

Balancing efficiency and trust

None of this diminishes the progress that integrated firms have made. In many situations, they deliver meaningful efficiencies in scheduling logistics and contracting and can be effective partners.

The key question organizations should ask is not, "Can one firm do both?" but rather, "What structure best reinforces stakeholder confidence?"

Efficiency is an important aspect of compliance programs, but specialization strengthens assurance outcomes. When these priorities conflict, governance considerations typically favor the latter.

KPMG's perspective

At KPMG, we recognize that cybersecurity assurance continues to evolve. The convergence of technology and risk management will undoubtedly continue, and collaboration across disciplines remains essential.

Leveraging decades of assurance experience and engagement with global enterprises, we believe the most resilient model aligns each engagement with the professional community best positioned to deliver it.

- PCI assessments benefit from deep technical cybersecurity specialized teams.
- SOC 2 examinations benefit from the rigor, independence, and methodological maturity of established CPA assurance practices.

Engaging separate firms is not about preserving professional boundaries for their own sake. It is about reinforcing the credibility, independence, and long-term trust that assurance reports are intended to provide.

Looking ahead

As cybersecurity assurance matures, organizations will continue refining how they demonstrate trust. The most successful programs will balance operational efficiency with institutional credibility.

Integrated providers will remain an important part of the ecosystem. Yet for organizations seeking the strongest governance posture and the most defensible assurance outcomes, specialization (leveraging distinct firms aligned to distinct disciplines) offers a durable advantage.

In an era where trust is both fragile and invaluable, thoughtful separation of assurance responsibilities may ultimately prove to be not an inefficiency, but a strategic safeguard.

Authors

Adam Brand
PCI Solutions Leader
T: 1 312 282 9878
20 Pacifica, Suite 700
Orange County, CA 92618

Nina Currigan
SOC Solutions Leader
T: 1 303 382 7808
1225 17th Street, Suite 800
Denver, CO 80202

Some or all of the services described herein may not be permissible for KPMG audit clients and their affiliates or related entities.

Learn about us: **kpmg.com**